世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6
G06F 12/14, G06K 19/07

A1

(11) 国際公開番号 WO99/08192

(43) 国際公開日 1999年2月18日(18.02.99)

(21) 国際出願番号 PCT/JP98/03505

(22) 国際出願日 1998年8月6日(06.08.98)

(30) 優先権データ
特願平9/212881 1997年8月7日(07.08.97) JP
特願平10/78212 1998年3月26日(26.03.98) JP

(71) 出願人（米国を除くすべての指定国について）
株式会社 日立製作所(HITACHI, LTD.)[JP/JP]
〒101-8010 東京都千代田区神田駿河台四丁目6番地
Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
宇佐美光雄(USAMI, Mitsuo)[JP/JP]
〒185-8601 東京都国分寺市東恋ヶ窪一丁目280番地
株式会社 日立製作所 中央研究所内 Tokyo, (JP)
(74) 代理人
弁理士 高橋明夫(TAKAHASHI, Akio)
〒103-0025 東京都中央区日本橋茅場町二丁目9番8号
友泉茅場町ビル 日東国際特許事務所 Tokyo, (JP)

(81) 指定国 CN, JP, KR, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

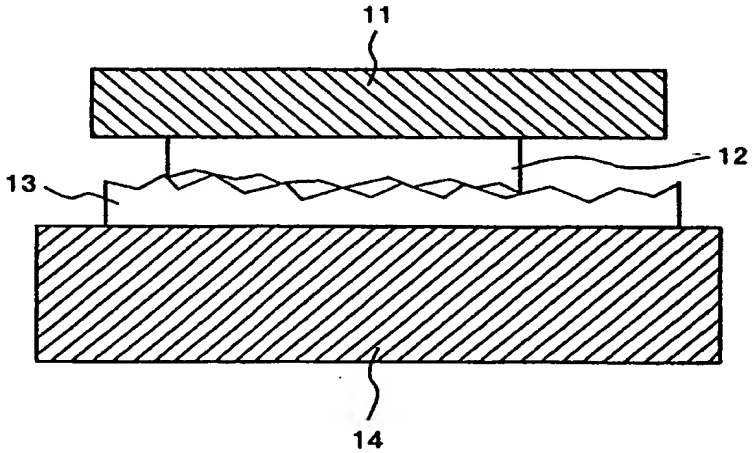
添付公開書類
国際調査報告書

(54)Title: SEMICONDUCTOR DEVICE

(54)発明の名称 半導体装置

(57) Abstract

A semiconductor device for effectively preventing forgery or alteration of IC cards or the like handling important information, comprising electrodes (12, 13), each having an unshaped irregular surface and provided, respectively, on the IC chip side and the substrate side, wherein the electrodes are connected to each other, with the IC chip (11) facing downward and the connection resistance is employed as a key code by subjecting the capacitance between the electrodes to A/D conversion, thus preventing the duplication of IC cards or the like by employing the connection resistance having a random value as the key code of cryptograph.



(57)要約

重要な情報を取り扱うＩＣカード等の偽造変造を防止する有効な手段を提供することをも目的とし、表面が不定形の凹凸を持つ電極１２，１３をＩＣチップおよび基板側にそれぞれ持ち、ＩＣチップ１１をフェースダウンでそれぞれの電極同士を接続して、その接続抵抗をその間の容量をＡ／Ｄ変換して、鍵コードとする。接続抵抗がランダム値となり、暗号の鍵コードとして使用することにより複製ができなくなる。

明細書

半導体装置

技術分野

本発明は、偽造や変造を防止した半導体装置、特にＩＣカードに関する。

背景技術

従来のICカードの偽造変造技術に関しては、プロセッシング オブ ザ セカンド ワークショップ オン エレクトロニツク コマース(「Proceedings of the 2nd Workshop on EIectronic Commerce, Oakland Ca1ifornia, Nov. 18-20, 1996」)に開示されている。

上記文献に示された偽造防止技術では、ICカードのチップ内に、取扱いが限定されるような、いわゆる鍵の役割をする鍵コードが記憶されている。この鍵コードはサービス(例えば、公衆電話やゲーム、通信等)を受けるときの課金すべきユーザのIDとして使われるもので、例えばクレジットカードの番号に対応するものである。それぞれのサービスシステムはIDを有するユーザの金融機関から、サービスに応じて料金を引き落とす。また、この鍵コードはユーザの信用チェックにも用いることが出来る。

この鍵コードはメモリエリアに格納されているが、第3者により読まれてしまうと、同類のカードが偽造変造されてしまう。なお、ICカードは、リーダ・ライタと接触してデータのやり取りを行う接触型と、無線技術によりデータをやり取りする非接触型とがある。いずれも、ICカードの中にはメモリエリアと、このメモリエリアへのデータのやり取りをする入出力エリアとを

有している。この入出力エリアにはプロセッサ回路が設けられており、複雑な暗号処理が可能である。

さて、このメモリエリアに格納されている鍵コードは、ICチップを電気的、物理的、または化学的に分析されて読まれてしまう危険性がある。鍵コードはメモリエリアのメモリセルに電気的に記憶されている。すなわち、メモリセルは電子(電荷)をチャージすることにより記憶を保持している。そのため、例えば電子顕微鏡の分解能を上げることによってパターンとして読み取ることが出来る。また、微細加工装置を使用することにより、メモリエリア周辺を加工して周辺回路に接続される配線を露出させ、メモリの周辺回路そのものを駆動してメモリセルの内容を読み取ることも出来る。

このようなコード読み出しを防止するために従来技術では、電池を常備して、何らかの電気的、物理的、化学的操作がICチップにアタックが加えられると電池による機能で、電源ダウン等でメモリが消えてしまう方法であった。

例えば、電池を使用すれば、ICカードのチップ周辺に分解的なアタックを検出するセンサを設け、このセンサの出力に連動してメモリ内容を消去するような回路を動作させることが出来る。メモリセルとしてSRAMを用いれば、ICカードが分解されたときに電源がオフしてメモリの内容は消えてしまう。

また、偽造等の防止のためコードを形成する従来技術は、例えば特開昭59－10937に開示されている。これは偽造等に対する安全性を高めるために、アンテナの共振周波数並びにその返送波の振幅と位相偏差を測定し、測定値を秘密保持すべきアルゴリズムに従つてこれらに対応する数値に変換され、この数値と秘密保持されるべき番号とを結合してコード番号として記憶させるものである。

このコード番号はICチップのメモリエリアの中に永続的に記憶される。

従来の電池を用いて偽造を防止する技術では、個々のICカードに電池を備えることになりICカードのコストが増大する、また、ICカードの使用期間が電池の寿命に依存する、衝撃による電池の破損や接点不良により信頼性が低下する、電池の薄膜化が困難でありICカードが厚くなる等の問題があり、実用化を阻害している。

また、電気的な諸性質に基づいてコードを決定する従来技術では、例えば、ばらつきの対象として電気回路の特性ばらつきを用いた場合には、ばらつきの範囲が狭く偽造されやすいこと、特性ばらつきは外部から容易に測定できること、集積回路の分解による解読に対して配慮がないことなどにより偽造に対して、不十分であった。

本発明の目的は、低コストで信頼性の高い、偽造変造防止方法及びそれを用いた半導体装置を提供することにある。

発明の開示

上記目的は、表面が不定形の凹凸を持つ電極をICチップおよび基板側にそれぞれひとつまたは複数個持ち、ICチップをフェースダウンでそれぞれの電極同士を接続し、その接続抵抗をアナログ／デジタル変換して、鍵コードとすることにより達成される。

すなわち、電極表面が不定形の凹凸のため接続されていた電極を一度引き離すと、離す前と同じ接触状態とすることはできないため、破壊的アタックの有つたことを推定することが可能である。

また上記目的は、ICチップおよび基板側にそれぞれひとつまたは複数個の

電極を持ち、ICチップをフェースダウンでそれぞれの電極同士を導電性接着剤で接続し、その接続抵抗をアナログ／デジタル変換して、鍵コードとすることにより、より効果的に達成される。

すなわち、導電性接着材によりアナログ量である抵抗値がより不定状態となり、接触抵抗のばらつきが拡大される。

さらに上記目的は、ICチップおよび基板側にそれぞれひとつまたは複数個の電極を持ち、ICチップをフェースダウンでそれぞれの電極同士を導電微粒子を含んだ異方導電接着剤を用いて接続し、その接続抵抗をアナログ／デジタル変換して、鍵コードとすることにより、より効果的に達成することができる。

すなわち、異方導電性接着材では接着剤の中に金の微細粒子(５～１０μm)の分散状態があって、電極間に挟まれて抵抗値をばらつかせる働きがある。

上記電極の材料と異方導電性接着剤の導電微粒子の材料との主成分を同じくすることにより、より大きな効果がえられる。

また上記目的は、表面が不定形の凹凸を持つ電極をICチップおよびシート側にそれぞれひとつまたは複数個持ち、ICチップの上にシートをかぶせてそれぞれの電極同士を接続して、その接続抵抗をアナログ／デジタル変換して、鍵コー ドとすることにより達成される。

すなわち、従来のフェースアップのICカード用チップであっても表面にシートを貼ることにより、ICチップのプロセスをそのまま用いることができるので低コストで実現できる。

上記目的は、上記アナログ／デジタル変換されたコードがＩＣカード外に読み出され暗号処理されて再び当該のICカードのICチップのメモリエリアに

書き込まれることにより、より効果的に達成される。

すなわち、正当な手続きによってなされた変換コードがチップ内に書き込まれていれば正しいカードと認識することができる。

上記目的は、アナログ／デジタル変換されたコードがICカードの当該チップ内で暗号処理されてICカード外に読み出され暗号処理されて再び当該のICカードのICチップのメモリエリアに書き込まれることにより、より効果的に達成される。

すなわち、ICチップ内で暗号処理されることにより、ラインモニタによってデータが読まれても、ICチップの鍵コードを読まれることがないので安全性が増加する。

上記目的は、生成されたICカードの鍵コードがリーダライタによって読み取られデータベースにICカードの登録コードとともに保存されることにより、より効果的に達成される。すなわち、ICカードはシステムのサポートにより実用化されるが、ICカード上の鍵コードがシステムのデータベースに登録されていると、安全に運用し、認証システムに使用することが可能となる。なお、登録コードとしてはIDナンバー、名前、暗証ナンバー、個人の属性データ、サービスの来歴データ、クレジットナンバー、口座情報、信用レベルなどがある。

上記目的は、生成されたICカードの鍵コードがICカードの偽造および変造を防止するために用いられることにより、より効果的に達成される。

すなわち、鍵コードは接触抵抗のばらつきによって実現されるので、同じ鍵コードとなる確率は極めて小さく、同じカードを作ることは極めて困難である。

上記目的は、生成されたICカードの鍵コードがICカードとリーダライタとの相互認証を行うために用いられることにより、より効果的に達成される。

すなわち、本発明で使用される鍵コードは再現が極めて難しいので、相互認証のために用いることができる。

上記目的は、生成されたICカードの鍵コードが暗証コードまたは生物的特徴コードと結び付いて、本人認証を行うために用いられることにより、より効果的に達成される。

すなわち、人体の特徴をICカードの中のコードに鍵コードと一緒に記憶すると、偽造が難しい、その人固有の個人認証カードを提供することができる。

上記目的は、コードとして生物的特徴コード(掌紋コード、指紋コード、匂いコード、顔コード、音声コード、静脈コード、瞳孔コード、DNAコード)を用いることにより、より効果的に達成される。

すなわち、上記バイオメトリクスで考えられるその人の個人コードを用いることにより．個人認証を安全に実現することができる。

上記目的は、公開鍵暗号の解読や共通鍵暗号の解読がリーダライタではなく、上位のシステムで行われことにより、より効果的に達成することができる。

すなわち、多数設置されているリーダライタでクローズして行われると、リーダライタが第三者に分解されて暗号システムが解読される恐れがある。数の少ない上位システムで厳重に管理することによりこの危険を低減することができる。

上記目的は、生成された鍵コードが電子マネーとしてICカードが使用されるときの本人認証や偽造チェックやICカードとリーダライタの相互認証に使

用されることにより、より効果的に達成される。

すなわち、安全にIDが行われると、課金システムなどへの応用が可能となり、電子マネーとしてICカードを使用することが可能となる。

上記目的は、アナログ／デジタル変換の分解能が4段階以下であることにより、より効果的に達成される。

すなわち、分解能を4段階以下に押さえることにより経時的な接触抵抗の変動があっても信頼性よく再現することができる。

上記目的は、一つの電極同士の接続部分のサイズが１５ミクロン以下であることにより、より効果的に達成される。

すなわち、電極を複数の小パッドアレイとすることにより、小面積で安全性の高い鍵コードを経済性よく提供することができる。

上記目的は、複数の電極同士の接続部分がマトリクス状に配列されていることにより、より効果的に達成される。

すなわち、コンパクトな接続アレイを提供できる。

上記目的は、生成された鍵コードが複数のカードが同時に応答したとき判別するためのコードとして使用されることにより、より効果的に達成される。すなわち、同一の鍵コードがほとんど存在しないので複数のカードを認識するためのコードとして使用することができる。

上記目的は、表面が不定形の凹凸を持つ電極をICチップおよび基板側にそれぞれひとつまたは複数個持ち、ICチップをフェースダウンでそれぞれの電極同士を接続して、その接続抵抗をアナログ／デジタル変換するとき、アナログ値が境界領域にあるものを回避することにより、より効果的に達成される。

すなわち、A/D変換するとき、アナログ値からデジタル変換の境界にあると、経時変化によってデジタル値が変動する恐れがある。従つて境界にあるものは使用しないか、境界値を変化することによって信頼性を増すことができる。

さらに、上記目的を達成するための本発明のＩＣカードは、互いに対向して配置された 基板および半導体チップと、当該墓板および半導体チップの互いに対向する側の表面上にそれぞれ互いに対向かつ離間して配置された電極を有し、当該電極間に形成された容量の容量値が数値化されて、ICカードの鍵コードとして使用される。

すなわち、本発明においては、それぞれ互いに対向かつ離間して配置された電極間に形成された容量の容量値を数値化し、この数値化された容量値がICカードの鍵コードとして使用される。上記容量値は、ランダムに異なっており、しかも公開鍵のアルゴリズムに従つて暗号化されているため、第三者によってICカードが偽造や変造される危険は極めて少ない。

上記半導体チップには増幅器が形成されており、当該増幅器に接続された上記容量および所定の抵抗によって積分回路が形成され、上記容量値の数値化は、この積分回路によって出現された電圧値をアナログ・デジタル変換することによって行われる。上記増幅器のみではなく、上記抵抗も上記半導体チップにあらかじめ形成しておくことができることはいうまでもない。

上記基板および半導体チップの上にそれぞれ複数個の上記電極を形成し、互いに対向かつ離間して配置された上記電極の間に形成された容量の容量値が、ランダムに異なっているようにすることができる。このように容量値がランダムに異なっていれば、たとえある一つの容量値が第三者に知られても、

他の容量を知られる恐れはほとんどなく、第三者によるＩＣカードの偽造や変造が極めて困難である。

このような容量値がランダムに異なっている容量は、例えば、上記互いに対向かつ離間して配置された各電極の間に、異なる種類の誘電体からなる誘電体膜を介在させる、同じ種類の誘電体からなり厚さが互いに異なる誘電体膜を介在させる、および上記互いに対向かつ離間して配置された電極の間の距離が互いに異なるようにするなどの手段を用いて形成することができ、電極の間の距離が互いに異なる構造を実現するための一手段としては、上記互いに対向かつ離間して配置された電極の厚さが互いに異なるようにすればよい。

上記容量値がランダムに異なる容量を形成するには、種々な手段を用いることが可能であり、例えば互いに対向かつ離間して配置された上記電極の間に、直径が互いに異なり、かつ同一種類の粒子状の誘電体を介在させてもよい。

本発明において、上記互いに対向する電極の間に介在する誘電体膜としては、$BaSrTi0_3$膜、PZT膜、$CaTI0_3$膜および$KHZP0_4$膜からなる群から選ばれた膜を使用することができる。

本発明によってICカードの正否を判定するには、下記の方法によって行うことができる。すなわち、まず、名前エリアと鍵コードが形成された半導体チツフを有するICカードに、当該ICカードの所有者の名前を、リーダライタによって問い合わせる。これに対して上記ICカードは、所有者の名前をリーダライタに回答し、リーダライタは、この回答にもとづいてデータベースに上記名前を送つて鍵コードを問い合わせる。リーダライタは、さらに乱数を

用いて公開鍵コードを発生させてこれを上記ICカードへ送り、ICカードは上記容量値を数値化して得られたランダム数値を暗号化してリーダライタに回答する。リーダライタは上記ICカードからの暗号化された回答を解読し、上記データベースの鍵コードと対比することによって上記ICカードの正否を判定する。

容量値がランダムに異なる容量にもとづいて鍵コードが形成され、しかもICカードによって暗号化されるので、第三者によって鍵コードが判読される恐れはほとんどない。

上記データベースには、上記使用者の名前とともに上記ICカードの鍵コードの数値をあらかじめ登録しておく。

本発明において、容量値がランダムに異なる容量を形成するには多くの方法を用いることができるが、最も代表的な方法は容量の誘電体膜の厚さや種類を変える方法である。厚さがランダムに異なる誘電体膜を形成するには、例えば周知の方法によってBST膜など誘電体膜を形成した後、レーザ光を照射する。レーザ光の強度をランダムに変えて走査を行えばランダムに程度が異なる蒸発(気化)が行われ、厚さが部分的にランダムに異なる誘電体膜が得られる。また、粒状の誘電体膜を両電極の間に介在させて、両電極の間にランダムに異なる圧力を印加しても厚さがランダムに異なる誘電体を得ることができる。

図面の簡単な説明

第１図は、本発明の第１の実施例を示す断面図である。第２図は、本発明の実施例(平面図)を示す図面である。第３図は、本発明の実施例を示す図面

である。第４図は、本発明の実施例を示す図面である。第５図は、本発明の実施例(断面図)を示す図面である。第６図は、本発明の実施例(平面図と断面図)を示す図面である。第７図は、本発明の実施例を示す図面である。第８図は、本発明の実施例を示す図面である。第９図は、本発明の実施例を示す図面である。第１０図は、本発明の実施例を示す図面である。第１１図は、本発明の実施例を示す図面である。第１２図は、本発明の実施例を示す図面である。第１３図は、本発明の第２の実施例を示す断面図である。第１４図は、本発明の第３の実施例の平面及び断面構造を示す図である。第１５図は、本発明の第４の実施例の平面及び断面構造を示す図である。第１６図は、本発明の第５の実施例を示す図である。第１７図本発明の第６の実施例を示す図である。第１８図は、本発明の第７の実施例を示す断面図である。第１９図は、本発明の第８の実施例を示す図である。第２０図は、本発明の第９の実施例の平面及び断面構造を示す図である。

発明を実施するための最良の形態

＜実施例１＞

第１図を用いて本発明の一実施例を説明する。ICカードの基板１４上には基板電極13が形成されている。一方ICチップ11 にもチップ電極12が形成されており、これら電極12、13の表面には不確定な凹凸面が形成されている。このような表面を持つ電極同士が密着すると、凸の部分が不規則に接するので導通抵抗は表面の状態と繋がった状態により、ランダムな値を示す。ここで、凹凸は±lnm～±100μmの大きさを有する。

この状態の接触抵抗値をアナログデジタル変換すれば、1から約10ビット

の情報量を得ることができる。すなわち、A/D変換のビット数であって、例えばオン／オフであれば1ビット、抵抗値を10ビットの精度でデジタル変換すれば1 0ビットのデータを得ることができる。

電極は複数個もつことを妨げないので、大量のランダムパターン(A/D変換した後の抵抗値のばらつき)を電気的に容易に得ることが可能であり、同一のパターンを得ることはきわめてまれであって、実用上は再現しない程度である。なお、計測器の精度が良すぎると抵抗値は再現しない。また、温度変化による温度ドリフトはキャンセルするように設定する必要がある。

この方法によれば、いったん電極を分離してしまうと繋がった状態が分離するので、再度電極を接続しても、接続状態の再現がきわめて困難となる。すなわち、チップの分解が行われると、チップ上の各所で同様の非再現分離が行われるため、物理的、化学的チップ操作による偽造防止策として極めて有効である。この方法は、破壊が行われると、メモリが消えるとみなすことができるので、電池を必要としない、自爆型メモリと考えることができる。

第２図を用いて本発明をICカードに適用したときの実施例について説明する。この例では、IC力ード21のコーナにICチップ搭載部22設けており、ここに搭載されるICチップ24の中には、電極搭載部25とメモリエリア23が設けられている。電極搭載部25には複数の電極26が、異方導電性接着材中に含まれる導竃微粒子27を介して、前記電極26に対向して設けられたＩCカード基板側の電極(図示せず)に接続されている。導電微粒子27は電極の表面の凹凸を増幅させる役割を果たす。この導電粒子27による電極間の接続抵抗をアナログ／デジタル変換して、鍵コードとして用いる。なお、ここでは複数の電極を示したが、一つでもよい。また、ICカード基板に設けられた電極とICチッ

プの電極との接続は、ICカード基板に設けられた電極上にICチップをフェースダウンで位置合わせして接続する。このとき電極材料と異方導電性接着剤の導電微粒子の材料の主成分を同じ、例えばAuパッドではAu粒子、Alパッドではal粒子とすることにより、凹凸との増幅効果を高めかつ化学的または透過型観察によるメモリ内容の読みだしを防ぐことができる。従つて、このような方法をとれば、接続抵抗をA／D変換してえられる乱数のランダムパターンを容易に得ることができる。この鍵コードを発生する部分を小面積とし、かつ微小導電粒子のサイズを15ミクロン以下、望ましくは5から10ミクロンとすることにより、電極アレイをコンパクトに実現でき、さらに複数の電極同士の接続部分をマトリクス状に配列することにより、さらに小面積で(面積効率良く)電極を形成できる。

第３図を用いて第２図で示した電極での電極接触抵抗32を鍵コードに変換する方法を説明する。電極接触抵抗32に電流源31によって、電圧を発生させ、アンプ33で増幅し、A/D(アナログデジタル)変換器34でデジタル変換して、出力端子35に電圧信号を発生させる。この電圧信号を鍵コードとする。例えば、A／D変換器が9ビットであって、ＭＡＸ値が約１Ｖ、分解能が１mVとすれば、1～1023　mV、2進数で111111111(=1023)となる。アナログデジタル変換器34は当該電極の形成されたICチップの中に設けられる。

第４図を用いて鍵コードをICチップのメモリエリアに書き込む手順を説明する。アナログ／デジタル変換された鍵コードはリーダライタ(3WU)によりICカード外に読み出され、リーダライタ側で暗号処理される。例えば、鍵コード1 11111111が読み出され、暗号処理されて、例えば101010101となる。その後、暗号処理されたコード101010101が当該のICカードのICチップのメ

モリエリアに書き込まれる。

または、アナログ／デジタル変換されたコードは、リーダライタ側でなくICカードの当該チップ内で暗号処理されてICカード外に読み出され暗号処理されて再び当該のICカードのICチップのメモリエリアに書き込まれる。当該チップ内での暗号処理は公開鍵暗号処理とすれば、当該者のみA／D変換された内容を読むことが可能である。ここで、公開鍵暗号処理とは、鍵はオープンになって暗号化は誰にでもできるが戻すことができない暗号処理である。例えば、沢山の人から暗号化した文書をもらっても特定の人しか解読できない。

暗号化されたものまたは暗号化されないままのA／D変換の内容はカード読み取り器またはさらに上位のシステムによって、暗号化されて、再びICカードのチップに送り込まれて、ICチップ内のメモリエリアに書き込まれる。

暗号化されたものがさらに暗号化される例としては、まず自己の鍵で暗号化してそれを公開鍵で送る方法があり、相手からみると特定の人しかできない方法であり、電子署名が1例である。暗号化されていない内容が暗号化される例は、衛星放送やペイTVに使われており、スクランブルする暗号方式がある。

このメモリ内容は、例えば不揮発性メモリに書き込まれ、ICカードのID番号となる。このID番号は使用される毎に照合される。上記コードとして同じものを生成するのは実質不可能なのでこのコードをID番号として用いることができ、カードの正当性を示すことができる。

なお、A／D変換の値を模擬しても、上位のシステムでの暗号鍵が非公開であるためID番号を作成することができず、偽造は困難となる。すなわち、

メモリ内容は読むことは可能だが、乱数発生からA/D変換および暗号化の部分が再現できないので、偽造の場合にはシステムチェックで見出すことができる。

さらに、照合シーケンスによって、カードの照合が行われるので、変造されたカードはリジエクトされる。カード内にある接続抵抗をA／D変換した数値を読み出して、システム内の暗号鍵で暗号化したものと、カード内のメモリ内にあるコードを照合することにより、そのカードが正当なものか判断できる。

第５図により、電極間の接続に導電微粒子51を含む異方導電性接着剤を用いた実施例について説明する。電極の間に電極表面の凹凸よりも大きな導電微粒子が挟まれている。この導電微粒子はランダムに分散されており、電極表面に形成された凹凸と同様の役割をはたす。1μm以下の小さな凹凸や平坦性が高いもの同士では接触抵抗に差がでにくい。このとき、5～10μmφの導電粒子が存在すると導電粒子の変形の程度によってばらつきがでやすくなる。

また、電極の表面の状態、導電微粒子の表面状態、接続場所、接続時の変形、数量、電極の面積など、ランダムな抵抗値を発生する要因はさまざまである。この導電微粒子はプラスチック粒子にチタン金メッキしたものや、ニッケル粒子などさまさまな粒径およびその混在が可能である。この導電粒子は分散を維持したままエポキシ接着樹脂で強固に接着されるので、安定に接続状態が維持できる。

第６図は表面が不定形で±lnm～±100μmの間の大きさの凹凸を持つ電極をICチップおよびシート側にそれぞれひとつまたは複数個持ち、それぞれの電極が対向するようにICチップの上にシートをかぶせてそれぞれの電極同士

を接続し、その接続抵抗をアナログ／デジタル変換して、鍵コードとするICカードの実施例を示している。なお、シートとしてはPETを用いることができる。図 6(a)は平面図であって、ICチップ61の上にあるチップ電極65の上にはシート62が設けられている。このシートに設けられたシート電極63とチップ電極65とが接続されている。第６図(b)は第６図(a)のA—A'の部分断面図を示している。この構成は第１図と同じであって、いままでの実施例と同様に電極の表面の凹凸による接触抵抗のランダム性と分離時の状態消去を利用している。

なお、シートと当該ICチップの一部には貫通電極64が設けられており、凹凸のある電極間の接触抵抗がモニタできる。ここでは、電極の接続が互いに一つずつであるが、第２図に示したように複数個であってもよい。第６図に示した構造とすることにより、通常のフェースアップして実装し、ワイヤボンデイングするICカードでもこの偽造防止技術を適用することができる。すなわち、ICチップの実装方法によらずどのようなＩＣカードでも、接続抵抗の情報を用いた鍵コードを備えることができる。シートを用いた本技術により、安全にICカードの利便性を享受可能となる。

第７図は本発明による鍵コードを使用して、当該のICカードが偽造されたものでないことを確認するためのフローを示すコICカードを適用したシステムでは、運用対象とする金額が磁気カードと比べて格段に多額であるため、(1) IC カードの使用者本人確認、(2)ICカードの偽造されたものかの確認、(3) ICカードの正当性をみるためにリーダライタ(システム)との相互認証が必要である。本発明では(1)-(3)全ての確認が可能となる。

第７図のフローは(2)の偽造確認である。まず、ICカード内チップ小パッド

の接続抵抗A／D(アナログデジタル)変換した鍵を公開鍵暗号処理してリードライタで読み取りを行う。鍵は乱数的に発生されるので、この鍵コードは一義的に与えられ同一の鍵コードをもつICカードが存在することはきわめてまれである。

またこの鍵コードは微小部分の接触抵抗をA／D変換したものであって、ICカード内部の微細素子と配線によってデジタル変換されるので、ICチップに接触して、直接電気的方法でみることは極めて困難である。

ただし、デジタル変換された鍵コードがリーダライタの問い合わせに対してそのままのビット列で読みだされるとラインモニタされて、第3者に容易に鍵コードが得られてしまい機能を失つてしまう。そのために、ICカードに公開鍵を与えてICカード内で当該の鍵コードを暗号化して、ICカードから暗号化された情報を得ることにより、ラインモニタされても当該の鍵コードが読まれないようにする。

次に、鍵コードを解読して共通鍵暗号方式でたとえば2,000ビット共通鍵で暗号化しておく。これをAとする。次に、当該のICカード内のメモリエリア内にあるデータをそのまま読みだす。これをBとする。AとBが一致すれば、当該のICカードは偽造されたものではないと確認できる。

このとき、公開鍵暗号の解読や共通鍵暗号の解読をリーダライタで行うことができる。さらに、この解読を上位のシステムで行うことにより、リーダライタ内に公開鍵や共通鍵をおいて暗号解読した場合にリーダライタが分解されてシステムのセキュリティが被られる問題を対策できる。

このように、ICカード内で本発明の方法によって生成されたICカードの鍵コードはICカードの偽造および変造を防止するために用いることができる。

第８図は上記(.3)で示したICカードとリーダライタとの間の相互認証のフローを示したものである。実施例として2つの方法を示す。第８図(a)に示した第一の方法では、まず、当該ICカード内のチップ小パッド(ワイヤボンデイングなどパッドに比べて小さなパッドで100μm以下)の接続抵抗をアナログ／デジタル変換した鍵コードをICカード内で公開鍵暗号処理して、リーダライタで読み取る。リーダライタ側では、この鍵コードを解読して、システムに存在するデータベースから当該のICカードの鍵コードを読みだし、一致すれば相互認証完了とする。データベースには、ICカードの使用コーザの鍵コードが登録されており、更に鍵コードに付随してユーザの各種データ、ロギング記録(何時、何に、いくら、何処で使用したか等)が記録されている。システムで管理される鍵は、厳重に管理されている。

第二の方法を第８図(b)で説明する。まず、リーダライタ内のMPU(マイクロプロセッサ)の乱数アルゴリズムを使用して乱数を作り、ICカードに乱数を与えてICカード内チップ小パッドの接続抵抗をアナログ／デジタル変換した鍵コードで暗号化した情報を当該のリーダライタに送り返す。当該リーダライタでは、乱数を発生した後、リーダライタにLANや無線、インターネットで接続されているアプリケーションシステムのデータベースから獲得した鍵で同じ乱数を暗号化した情報を作成して先の情報と照合して一致すれば相互認証完了とする。

第９図を用いて複数の無線式のICカードを一つのリーダライタで読むときにそれぞれのICカードを判別する方法を説明する。本発明では同一のIDコードが付与されることが極めて少ないため、このIDコードを有効に活用することができる。IC力ード91はICチップ92が搭載され、このチップは鍵コード発

生 部93を有している。一方、他のICカード94の中には他のICチップ95が搭載されており、同様に鍵コード発生部分96を有している。それぞれの鍵発生部分の鍵コードは異なっているので、この鍵コードをIDコードとして用いることによりICカード91と94を区別することができる。鍵コードはビット数を増やすことによってID数を際限なく増やすことができるので、無限に近いICカードを区別することができる。

第１０図は本発明による鍵コードを有するICカードのためのシステム構成を示している。システムは、ICカード102とリーダライタ101およびデータベース107を有する。動作シーケンスをもとに、各機能部分を説明する。まず、

(1)リーダライタ側からICカードに対して、当該カードの管理責任者を特定するための名前コードまたは認識コード104を問い合わせる。この名前コードまたは認識コード104はICチップ103の中にあるメモリの所定のエリアに格納されている。なお、リーダライタはカードの存在をLEDセンサにより検知できる。カードへの電源供給は、非接触式カードの場合電磁波によりなされる。また、カードが正常に動作できる状態かどうかは、最初にリセット信号をリーダライタに送ると、ICカードの状態が分かるようなコード(アンサーツーリセット)をICカードからリーダライタへ返送することによりチェックする。また、ＩCカードの電源をオンにしてリセット状態にし、リードコマンドをアドレス付でICカードへリーダライタから送ると、名前コードがICカードからりーダライタへ送られる。これにより、名前コードを確認することができる。次に、

(2)ICカードは名前コード104をリーダライタ101に返答する。すなわち、リーダライタからのコマンドにより、ICカード内の回路が動作し、メモリから

名前コードを読み取りそのリーダライタへ名前コードを返答する。

(3)リーダライタはデータベース107にあるデータベース上の名前コード108を検索して、データベース上の鍵コード109を獲得する。なお、リーダライタは名前コードが記憶されたメモリアドレスを指定し、リードコマンドにより名前コードを読み出す。また、カードが複数存在する場合には輻輳制御により一つのカードが選ばれる。なお、輻輳制御とは、カードに対して各ビットの端から "0"、"1"をきいていって複数のカードの中から1つのカードを選択する制御法で、複数のカードが同時に応えないようにするものである。

(4)リーダライタは乱数をICカードへ送る。この乱数は、例えばリーダライタ内のMPUで回路的に発生される。LANやインターネットでサーバ側から乱数を供給してもよい。

(5)ICカードは、乱数を受け取つた時点でコマンドによってリーダライタから指示を受け、乱数を鍵コード発生部105に従つて発生した鍵コードによって暗号化した乱数を作成する。一方、リーダライタはICカードと同様にデータベースから得た鍵コード106を使用して、ICカードへ送つたのと同じ乱数を暗号化する。これによって得られた暗号化された乱数の結果と先のICカードからの暗号化された乱数を照合して、一致がとれれば、ICカードとリーダライタの相互認証が完了して、ICカードの正当性が認められる。なお、リーダライタはLAyやインターネット、回線等でサーバと接続されている。当該サーバ内にはデータベースが設けられている。また、サーバには複数のリーダライタが接続される。

生成されたICカードの鍵コード(IDコード)は、名前コードまたは認識コードとともにデータベースに格納される。

また生成されたICカードの鍵コード(IDコード)は、ICカードとリーダライタとの相互認証に用いられる。また生成されたICカードの鍵コードは暗証コードまたは生物的特徴コードと併用して、本人認証を行うために用いることができる。

生物的特徴コードは、手のひらをパターン化した掌紋コード、指紋をデータ化した指紋コード、人体から発生する匂いに基づく匂いコード、顔の形をパターン化した顔コード、声の情報をパターン化(デジタル化)した又は分析値に基づく音声コード、静脈のパルスをパターン化した静脈コード、目の色や形をパターン化した瞳孔コード、DNAの情報をパターン化したDNAコードを用いることができる。

生成された鍵コードは電子マネーとしてICカードが使用されるときの本人認証や偽造チェックやICカードとりーダライタの相互認証に使用することができる。これにより、他人にカードを無断で使用される恐れがなくなり、財産や個人情報の管理を安全に行うことができる。

上記システムは、例えば、一般商店での支払い、チケットの購入、定期券での改札、免許証のチェック、テレフォンカードによる電話等々多くの分野(交通、運輸、金融等々)に応用することができる。これにより、商店ではカードをかざすだけで商品を買うことができる。また、映画館に行くときその都度並んで切符を買うことなく入場できる。旅館の予約や精算ができる。インタネットで雑誌の必要な部分だけをコピーして料金を払うことができる。有料放送TVで所望の放送を鑑賞できる。マンツーマンの英会話の料金支払いができる。クレジットカードの代わりに使え、かつ小金の決済にも使える。更に、コンピュータシステムや場所のアクセスにも使うことができる。

第１１図は本発明を適用した非接触ICカードの構成例を示す。ICチップ111は非接触ICカード」13の厚さ方向においてほぼ中立面にあり、カードのほぼ中立面に形成されたコイルパターン112と接続されている。コイルパターンのクロスオーバする部分は絶縁膜114があって、ショート防止を図つている。

第１２図はICチップの凹凸のある電極と基板上の凹凸のある電極を接続し、その間で発生する接触抵抗の特性を示している。横軸に接触抵抗部分に流す電流を示しており、縦軸に発生する電圧を示す。ここでは一例として4本の代表特性が示されているが、これらの特性は極めてランダムに発生するので、複数ある電極間の抵抗値の特性はそれぞれ異なる。なお、電流値として0.1～lmAの範囲の値を使うと電圧値に差がでやすい。

本発明はこのような特性のバラツキを活用するものであるが、アナログ／デジタル変換するとき分解能は任意に設計することを妨げるものではない。ここで、

分解能を4水準に分けることにより再現性よく抵抗値を得ることができ、効果的である。電極のサイズを1～15μm角とし、この上に接触抵抗のばらつきを増大させるような要素(異形状の粒子など)を配置し、対向する各電極との間の抵抗値を電流を流して電圧変換する。 この電圧値を2ビットのA/D変換器でデジタル化することにより容易に4水準を得ることができる。すなわち、00、01、10、11のパターンとなる。

これは接触抵抗は表面の状態に従つて決定されるので．経時的変化に対して対応しておく必要があり、これを信頼性よく実現するためには、必要以上に分解能を上げず、余裕をもたせることにより安定性が増すためである。分

解能は接続抵抗値を電圧変換し、それをA/D変換するときの回路の精度で決まるものであるが、温度ドリフト、ストレス、経時変化により再現性が劣化する。分解能としては2～10000ぐらいの範囲の値を取り得る。

また、アナログ／デジタルの動作帯を設定して、境界領域の接触抵抗を安定ポイントにあるものを選択し、安定化を図る。ここで、境界領域とはデジタル化するときの境界であり、例えば10と11との間ということである。

アナログ／デジタル変換の分解能を4段階以下(2～4段階)とすることにより、より再現性が高くなる。また、生成された鍵コードを、複数のカードが同時に応答したとき判別するためのコードとして使用することにより信頼性と安全性に優れたICカードを提供することができる。

＜実施例２＞

第１３図は本発明の第２の実施例の断面構造を示　す図である。第１３図に示したように、本実施例では、半導体チツプ２１２上に形成された厚さ0.１～50μmのAuからなるチップ電極２１３と、厚さ0.１～1.0mmのＰＥＺからなる基板２１５上に形成された銀ペーストからなる基板電極２１４は、互いに対向して配置され、上記チップ電極２１３と基板電極２１４の間には、BST（$BaSrTi0_3$）からなる誘電体膜２１１が介在している。

上記チップ電極２１３と基板電極２１４の間の容量は、誘電体膜２１１の材質、厚さおよび平面積などに依存するが、この誘電体膜２１１としては粒状、液状あるいはゲル状など、種々な形状のものを使用することができる。本実施例では、粒状のＢＳＴ膜を誘電体膜２１１として用い、両電極２１３、２１４間に互いに異なる圧力を印加して、誘電体２１１の厚さと形状を変えることにより、容量の値が広い範囲でランダムに異なる容量を形成した。例

えば、上記粒状のBST膜の直径が1μm、圧力を印加した後の誘電体膜２１１の厚さが1000ｎｍ、電極面積$1X10^4 \mu m^2$であるときの、得られた容量値は４５ＰＦであった。

誘電体膜２１１を変形させて所定の値の容量を得た後、電極２１３、２１４および誘電体膜２１１を樹脂(図示せず)によって固定して確定した。なお、この樹脂は、両電極２１３、２１４間に誘電体粒子を分散させて誘電体膜を形成するための媒体として使用してもよく、また、あらかじめ誘電体膜２１１を電極２１３、２１４の間に形成した後、得られた構造を固定するために樹脂を注入してもよい。いずれの場合においても、広い範囲で容量の値がランダムに異なる容量を得ることができた。

本実施例では、上記のように粒状のBSTを変形させて誘電体膜を形成したので、断面形状の測定が困難である、誘電体膜の面積や厚さの変更や設定が容易である、および製造が簡単で容易であるなどの利点がある。

また、本実施例では、一つの誘電体膜２１１を電極２１３、２１４の間に固定したが、誘電体膜２１１を複数個用いてもよく、互いに異なる形状を有する誘電体膜を用いてもよい。また、各電極２１３、２１４をそれぞれ複数としても良く、電極２１３、２１４の面積が互いに異なっていても良い。いずれの場合でも、両電極２１３、２１４の間のＢＳＴ膜からなる誘電体膜２１１の厚さと面積を変えて、多くの容量値をランダム的に実現することができた。

＜実施例３＞

第１４図を用いて本発明の第３の実施例を説明する。第１４図（a）は本実施例を示す平面図であり、第１４図（ｂ）はそのA-A’断面図である。第１

の電極２２１および第２の電極２２２は、それぞれ第３の電極２２３と対向して配置されている。各粒子２２４、２２５はいずれもＢＳＴからなる誘電体粒子であるが、第１の電極２２１と第３の電極２２３の間には小さな粒子２２４が介在し、第２の電極と第３の電極２２３の間には、上記粒子２２４より粒径大きな粒子２２５が介在している。

上記粒子２２４、２２５は、周知のガスデポ法を用いて形成したので、流刑がランダムに異なっている。誘電率が等しく直径が異なっているのであるから、第１の電極２２１と第３の電極２２３の間の容量値と第２の電極２２２と第３の電極２２３の間の容量値は互いに異なる。各誘電体粒子の粒径がランダム的に分散しているので各電極ごとに異なる容量値がランダムに得られる。なお、容量が形成できるのであれば、各電極２２１、２２２、２２３の材質や形状は特に限定されることはない。

＜実施例４＞

第１５図を用いて本発明の第４の実施例を説明する。第１５図（ａ）は本実施例を示す平面図であり、第１４図（ｂ）はそのA-A'断面図である。

第１の電極２３１及び第２の電極２３２は、それぞれ第３の電極２２３と互いに対向して配置されている、。第１の電極２３１と第３の電極２２３の間には、小さな誘電体の粒子２２４が介在しているが、第１５図（ｂ）に示したように、第２の電極２３２が薄いため、第３の電極２２３と第２の電極２３２間野空隙は極めて大きく、そのため 両者の間には誘電体の粒子は保持されない。その結果、第２の電極２３２と第３の電極２３２間の容量は、第１の電極２３１と第３の電極の間の容量よりはるかに小さくなる。

各電極２３１、２３２の厚さはランダムに異なっているため、各電極２３

１、２３２と第３の電極２３３の間の空隙もランダムに異なっており、ランダムに異なる容量を各電極２３１、２３２に得ることができた。厚さがランダムに異なる電極２３１、２３２は、本実施例ではメッキ電極を形成した後に、レーザによって表面を除去する方法を用いて形成した。

なお、本実施例においても、各電極２２３、２３１、２３２はこれらの電極の間に容量が形成できるのであれば、材質、形状、及び寸法に特に限定はない。

＜実施例５＞

第１６図を用いて本発明の第５の実施例を説明する。 容量２４１は上記実施例１で得られたものであり、アンプ２４２は上記容量２４１と電気的に接続された半導体チップの中に形成されている。容量２４１は電気的にアンプ２４１に接続された抵抗と積分回路を形成して電圧値を出現し、この電圧値は、この電圧値はアナログ・デジタル変換されて数値化される。

上記のように容量２４１の値がランダムであるので、出現した電圧値およびこの電圧値をアナログ・デジタル変換して得られた数値もランダムである。また、容量値は積層された半導体チップと基板の縦の構造(積層構造)によって決定されているので、第三者によるICカードの分解などによって、この縦横造が破壊されたり、剥離されたりすれば、容量値の再現が不可能になることはいうまでもない。

＜実施例６＞

第１７図は本発明のＩＣカードを利用したＩＣカードによって、商品の購

入や決済 などを行うシステムの概念図である。ＩＣカード２５１の中には、半導体チップが配置され、この半導体チップには名前エリアおよび鍵コードが形成されている。

まず、リーダライタ２５２によつてＩＣカード２５１に対して所有者の名前を問い合わせ(ステップ(I))、この問い合わせに対して、ＩＣカード２５１は．名前Ａをリーダライタ２５２に答える(ステップ(2))。この名前Ａはリーダライタ２５２からデ-タベース２５３に送られ、鍵コードを問い合わせる。

次に、リーダライタ２５２は、乱数を使用して公開鍵コードを発生し、この公開鍵コードをＩＣカード２５１に送る(ステップ(3))。

ＩＣカード２５２は、本発明で実現されたランダム数値(ランダムな容量値を数値化したもの)を、上記公開鍵コードのアルゴリズムに従つて暗号化し、暗号化された鍵コードをリーダライタ２５２に返答する(ステップ(4))。リーダライタ２５２は上記暗号化された鍵コードを解読して、データベース２５３の鍵コードＢとの照会を行つて、一致すれば正当なエCカードと認識する。

鍵コードがランダムな容量値を数値化したものにもとずいており、しかも乱数を用いて発生された公開鍵コードのアルゴリズムに基づいて暗号化されているので、第三者によって偽造や変造される恐れはない。

データベース２５３の鍵コードＢには、予め、ＩＣカード２５１の鍵カードの数値を読み取つて登録しておく。また、ラインモニタによってシュミュしーションされる危険性は、公開鍵コードを乱数的に発生することによって防禦することができる。

<実施例７>

第１８図を用いて本発明の他の実施例を説明する。第１８図は、不正使用者がＩＣカードをアタックして、電気的に容量値を読み出そうとした際に、容量が破壊された状態を示している。容量値を読み出すために電極２１３、２１４の間に0.１～１Ｖ程度の高電圧が印加されると、誘電体膜２１１が部分的に破壊されてショートパス２６１が発生し、電極間２１３、２１４が電気的に短絡される。

このようになると、電極２１３、２１４の電位差がほぼ等しくなり、電極２１３、２１４の間の電気力線が消滅して、容量が生じなくなってしまう。従つて、容量の再現が不可能になり、ICカードを分解することによって鍵コードが読まれる危険はなくなる。

本実施例では、誘電体膜２１１が破壊された例を示したが、ＩＣカードの分解によって鍵カードが読解されるのを防止するためには、電極２１３、２１４間が等価的に等電位になるようにすればよい。したがって、例えば適当な回路等を電極２１３、２１４の間に設けてショートパスを形成する、などの方法を用いてもよい。

＜実施例８＞

第１９図は本発明の他の実施例の平面配置を示す図である。ＩＣカードの半導体チップ２７１の中には、上記実施例１によって形成された容量２７２が形成されている。ＩＣカードを偽造する意図を持った人が、半導体チップ２７１をプローブによって探索して、容量素子または周辺の積分回路やアナログデジタル変換器にアタックを開始して、鍵コードを読み出そうとする。このとき、プローブが接続されたことを、ＬＳＩアタックセンス回路が感知して、高電圧発生回路に信号を送つて動作させる。このようにすると、容量

素子２７２の両端には、耐電圧以上の高電圧が印加されて、容量を形成する電極内部またはその周辺においてショートパスが発生し、電極を構成するメタル材料がマイグレーションしてしまう。

このようになると、容量値の再現は不可能になって、鍵コードの読み出しはできない。半導体チップを破壊しても容量値の検出は不可能であり、ICカードが 偽造あるいは変造される恐れはない。

＜実施例９＞

本実施例は、容量の誘電体膜の厚さをランダム的に変えて、容量値がランダムに分散した容量を形成した例であり、第２０図を用いて説明する。第２図０(a)は本実施例の平面図、第２０図（ｂ）はそのA-A’断面図である。第１の電極２８１と第２の電極２８２は、それぞれ第３の電極２２３と対向して配置されている。第１の電極２８１と第３の電極２２３の間には、薄い誘電体膜２８３が介在し、第２の電極２８２と第３の電極２２３の間には、上記誘電体膜２８３より厚い誘電体膜２８４が介在している。

誘電体膜２８３、２８４の誘電体率は等しく、厚さが互いに異なるので、第１の電極２８１と第３の電極２２３の容量値と、第２の電極２８２と第３の電極２２３の間の容量値は互いに異なる。

本実施例では、レーザ加工によって各誘電体膜の厚さが、ランダム的に分散するように製造した。その結果、各容量ごとに容量値が異なり、容量値がランダムに分散した。

なお、本実施例においてもても、各電極２８１、２８２、２２３は、これらの電極の間に容量が形成できるのあれは、材質、形状および寸法に特に限

定はない。

産業上の利用可能性

本発明により、ICカードの偽造変造に対して有効に防御できる方法を経済的に提供することが可能となる。表面が不定形の凹凸を持つ電極をICチップおよび基板側にそれぞれ持ち、ICチップをフェースダウンでそれぞれの電極同士を接続して、その接続抵抗をA/D変換して、鍵コードとする。 一般に電極は複数個持つ。接続抵抗がランダム値となるので複製ができなくなる。

さらに対向して配置された半導体チップ側の電極と基板側の電極の間の誘電体膜の材料、厚さあるいは形状等を変え、容量値をA/D変換して鍵コードとすることによって、容量値はランダム的に分散した値となり、これを暗号化して鍵コードと使用するので、偽造や変造が不可能である。

またICカードを分解したり、電気的測定を行うと容量が破壊されて再現不能となるので、偽造や変造は不可能である。

請求の範囲

1. 第1の電極を備えたICチップと、前記第1の電極に対向して設けられ、前記第1の電極に電気的に接続された第 2の電極を備えた基板とを有し、 前記第1と第2の電極との接続抵抗をアナログ／デジタル変換した情報に基づき作成された鍵コードを備えていることを特徴とする半導体装置。

2. 第1の電極を備えたICチップと、前記第1の電極に対向して設けられ、前記第1の電極に導電性接着材を用いて電気的に接続された第2の電極を備えた基板とを有し、前記第1と第2の電極との接続抵抗をアナログ／デジタル変換した情報に基づき作成されたコードを備えていることを特徴とする半導体装置。

3. 第1の電極を備えたICチップと、前記第1の電極に対向して設けられ、導電微粒子を含んだ異方導電性接着材を用いて前記第1の電極に電気的に接続された第2の電極を備えた基板とを有し、 前記第1と第2の電極との接続抵抗をアナログ／デジタル変換した情報に基づいて作成されたコードを備えていることを特徴とする半導体装置。

4. 前記第1及び第2の電極の材料と前記導電微粒子の材料の主成分が同じであることを特徴とする請求項3記載の半導体装置。

5. 表面に不定形の凹凸を有する第1の電極を備えたICチップと、前記第1の電極に対向して設けられ、前記第1の電極に電気的に接続された第2の電極を備えたシート状基板とを有し、 前記第1と第2の電極との接続抵抗の値に基づき作成された鍵コードを備えていることを特徴とする半導体装置。

6. 前記鍵コードは、前記アナログ／デジタル変換された情報が暗号処理さ

れ、前記ICチップのメモリエリアに書き込まれたものであることを特徴とする請求項 1記載の半導体装置。

7． 前記鍵コードは、前記アナログ／デジタル変換された情報が前記ICチップ内での第1の暗号処理と、前記ICカード外での第2の暗号処理とがなされ、その後前記ICチップのメモリエリアに書き込まれたものであることを特徴とする請求項1記載の半導体装置。

8． 前記鍵コードは、前記ICカード用のリーダライタによって読み取られ、前記リーダライタに接続されたサーバ内に設けられたデータベースに前記ICカードの登録コードとともに保存されていることを特徴とする請求項1記載の半導体装置。

9．前記鍵コードは、前記ICカードの偽造および変造を防止するために用いられるものであることを特徴とする請求項1記載の半導体装置。

１０． 前記鍵コードは、前記ICカードと前記ICカードとの情報のやり取りを行うリーダライタとの相互認証を行うために用いられるものであることを特徴とする請求項1記載の半導体装置。

１１． 前記鍵コードは、暗証コードまたは生物的特徴コードと併用されて本人認証を行うために用いられるものであることを特徴とする請求項1記載の半導体装置。

１２． 前記生物的特徴コードは、掌紋コード、指紋コード、匂いコード、顔コード、音声コード、静脈コード、瞳孔コード、DNAコードの中から選択された少なくとも一つからなることを特徴とする請求項11記載のの半導体装置。

１３． 前記鍵コードの読み出しに用いる公開鍵暗号の解読や前記鍵コード

のメモリ書き込みに用いる共通鍵暗号の解読がリーダライタを制御する上位のシステムで行われことを特徴とする請求項6記載の半導体装置。

１４．前記鍵コードは、前記ICカードが電子マネーとして使用されるときの本人認証や偽造チェック、前記ICカードとリーダライの相互認証に使用されるもの であることを特徴とする請求項1記載の半導体装置。

１５．前記アナログ／デジタル変換の分解能は、2～4段階であることを特徴とする 請求項1記載の半導体装置。

１６．前記第1と第2の電極の接続部分のサイズが15ミクロン以下であることを特 徴とする請求項1記載の半導体装置。

１７．前記ICチップには複数の電極がマトリクス状に配列されていることを特徴とする請求項1記載の半導体装置。

１８．前記鍵コードは、同時に応答した他の複数のICカードと判別するために使用されるものであることを特徴とする請求項1記載の半導体装置。

１９．前記第1又は第2の電極の少なくとも一方は表面が不定形の凹凸を持つことを特徴とする請求項1の半導体装置。

２０．前記簾1および第2の電極はそれぞれ複数の小パッドのアレイからなることを特徴とする請求項1の半導体装置。

２１．前記アナログ／デジタル変換に際し、前記接続抵抗のアナログ値がビット切り替え部分である境界領域にあるものを回避する手段を有することを特徴とする請求項1の半導体装置。

２２．ICチップに設けられた第1の電極と前記ICチップとは異なる基板に設けられた第2の電極との接続抵抗を求める工程と、前記接続抵抗の値に基づいて情報コードを作成する工程と、前記情報コードを暗号処理する工程と、

暗号処理された前記情報コードを前記ICチップに記憶する工程とを有することを特徴とするコード作成方法。

２３．　上記暗号処理は、前記ICチップの外部で行われることを特徴とする請求項2 2記載のコード作成方法。

２４．　上記暗号処理は、前記ICチップの内部で行われる第1の暗号処理と前記ICチップの外部で行われる第2の暗号処理とを含むことを特徴とする請求項22記載のコード作成方法。

２５．　ICチップに設けられた電極と、基板上に設けられ前記電極に接続された電極との接続抵抗に基づく情報を読み取る工程と、前記ICチップに記憶されたコードを読み取る工程と、前記情報と前記コードとを照合する工程とを有することを特徴とする照合方法。

２６．　前記情報は、前記接続抵抗がアナログ／デジタル変換され公開鍵暗号処理された後、更に共通鍵暗号方式で暗号化されたものであることを特徴とする請求項25記載の照合方法。

２７．　前記公開鍵暗号処理は、前記ICチップ内で行われることを特徴とする請求項26記載の照合方法。

２８．　前記共通暗号方式での暗号化は、前記ICカード用のリーダライタ内で行われることを特徴とする請求項26記載の照合方法。

２９．　前記照合は、前記ICカードの偽造確認を目的とするものであることを特徴とする請求項2～28の何れかに記載の照合方法。

３０．　半導体装置に設けられた第1の電極と第2の電極との接続抵抗に基づく第1の情報を得る工程と、前記半導体装置を特定するために記憶された第2の情報をデータベースから得る工程と、前記第1の情報と前記第2の情報とを

照合する工程とを有することを特徴とする照合方法。

３１．　前記第1の情報は、前記接続抵抗がアナログ／デジタル変換され公開鍵暗号処理された後、解読されたものであることを特徴とする請求項30記載の照合方法。

３２．　前記照合は、前記半導体装置を認証するために行われることを特徴とする請求項30又は31記載の照合方法。

３３．　半導体装置に設けられた第1の電極と第2の電極との接続抵抗を求める工程と 前記接続抵抗をアナログ／デジタル変換した情報で乱数を暗号処理して第1の情報を得る工程と、前記半導体装置を特定するために記憶された情報をデータベースから読み取る工程と、　前記データベースに記憶された情報で前記乱数と同じ乱数を暗号処理し第2の情報を得る工程と、前記弟1の情報と前記第2の情報とを照合する工程とを有することを特徴とする照合方法。

３４．　前記照合は、前記半導体装置を認証するために行われることを特徴とする請求項33記載の照合方法。

３５．　互いに対向して配置された基板および半導体チップと、当該基板および半導体チップの互いに対向する側の表面上にそれぞれ互いに対向かつ離間して配置され た電極を有し、上記電極間に形成された容量の容量値を数値化したものが鍵コードとして使用されることを特徴とするICカード。

３６．　上記半導体チップには増幅器が形成されており、当該増幅器にそれぞれ接続された上記容量および所定の抵抗によって積分回路が形成され、上記容量値の数値化は、上記積分回路によって出現された電圧値をアナログ・デジタル変換することによつて行われることを特徴とする請求項３５記載のI

Cカード。

３７．　上記基板および半導体チップの上にはそれぞれ複数個の上記電極が形成され、互いに対向かつ離間して配置された上記電極の間に形成された容量は、容量値がランダムに異なっていることを特徴とする請求項３５若しくは３６記載のＩＣカード。

３８．　上記互いに対向かつ離間して配置された電極の間には、異なる種類の誘電体からなる誘電体膜が介在していることを特徴とする請求墳３７に記載のＩＣカード。

３９．　上記互いに対向かつ離間して配置された電極の間には、同じ種類の誘電体からなり・厚さが互いに異なる誘電体膜が介在していることを特徴とする請求項３７記載のICカード。

４０．　上記互いに対向かつ離間して配置された電極の間の距離が互いに異なることを特徴とする請求項３７記載のＩＣカード。

４１．　上記互いに対向かつ離間して配置された電極の厚さが互いに異なることを特徴とする請求項４０記載のＩＣカード。

４２．　上記互いに対向かつ離間して配置された上記電極の間には、直径が互いに異なり・かつ同一種類の粒子状の誘電体が介在していることを特徴とする請求項３７記載のICカード。

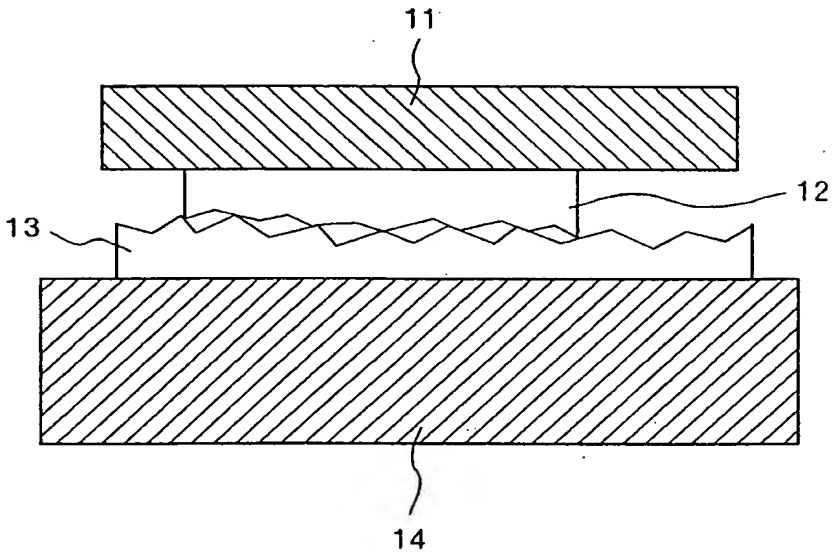
４３．上記誘電体膜は、$BaSrTiO_3$膜、ＰＳＴ膜、$CaTiO_3$膜、およびKH_2PO_4膜からなる群から選ばれることを特徴とする請求項３５～４２のいづれか一に記載のICカード。

４４．　名前エリアと鍵コードが形成された半導体チップを有するICカードに当該I Cカードの所有者の名前を問い合わせ、上記ICカードからの回答に

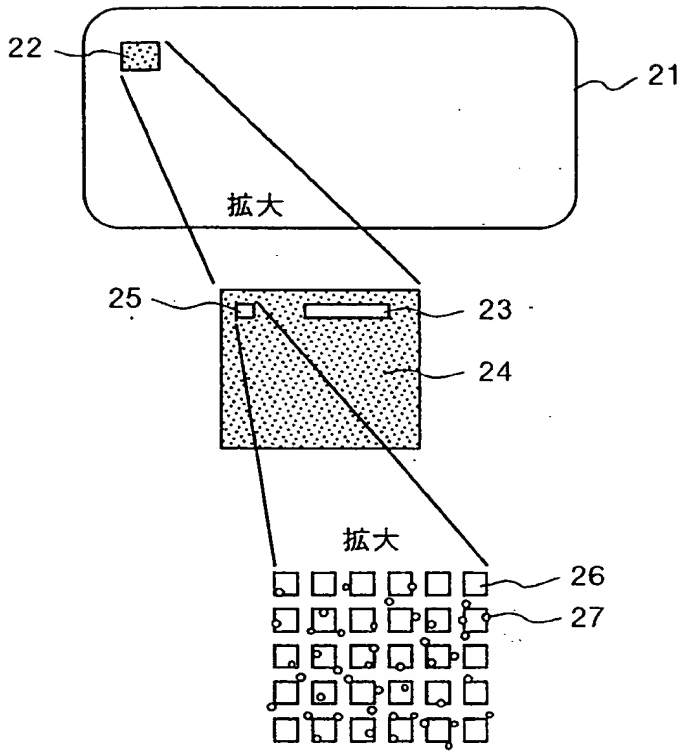
もとづいてデータベースに上記名前を送つて鍵コードを問い合わせ、さらに乱数を用いて発生させた公開鍵コードを上記ICカードへ送り、上記エCカードからの暗号化された回答を解読して上記データベースの鍵コードと対比することによって上記ICカードの正否を判定することを特徴とするＩCカードの正否判定方法。

４５．　上記データベースには、上記ICカードの鍵コードの値があらかじめ登録されていることを特徴とする請求項４４に記載のＩＣカードの正否判定方法。

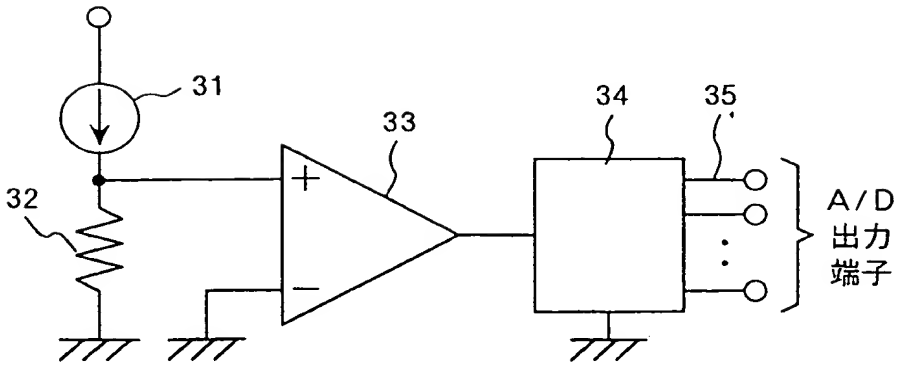
第１図



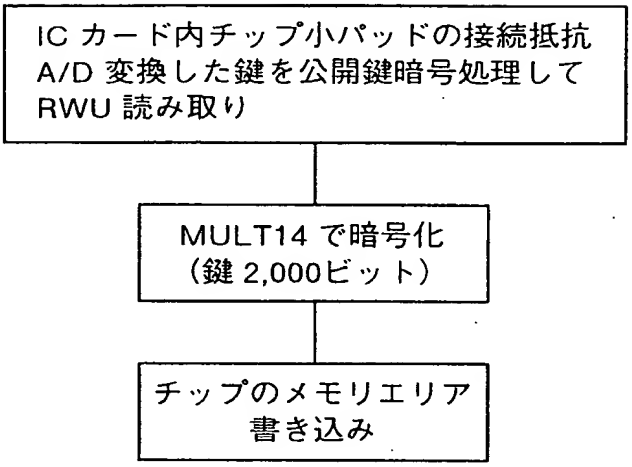
第２図



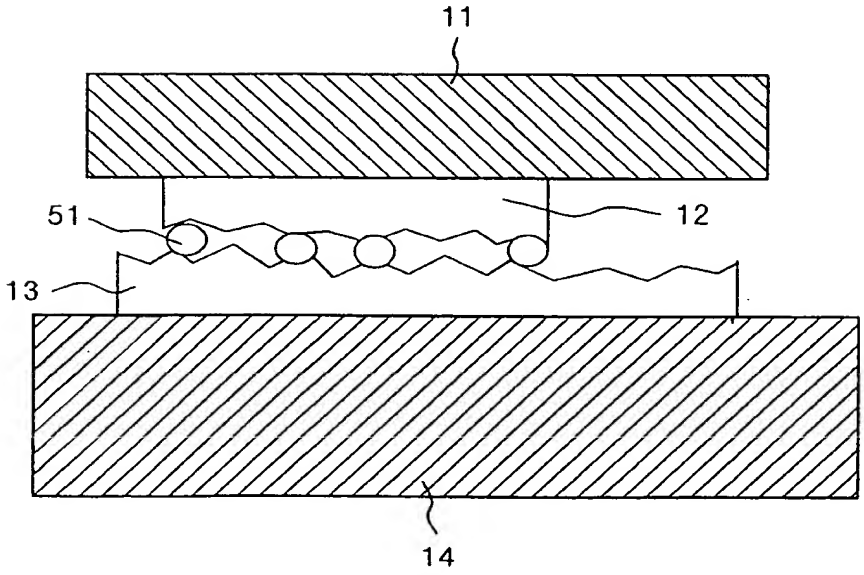
第３図



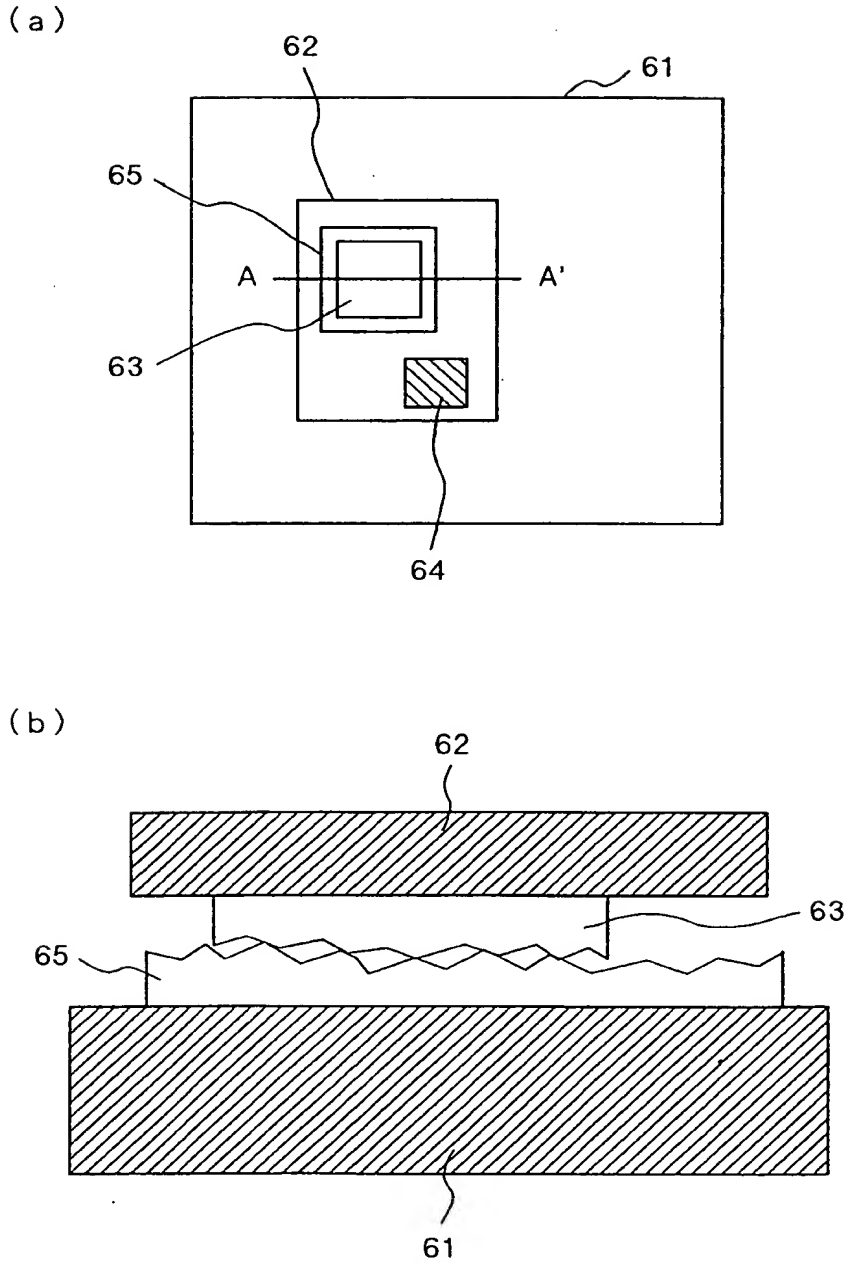
第 4 図


IC カード内チップ小パッドの接続抵抗
A/D 変換した鍵を公開鍵暗号処理して
RWU 読み取り
MULT14 で暗号化
（鍵 2,000ビット）
チップのメモリエリア
書き込み

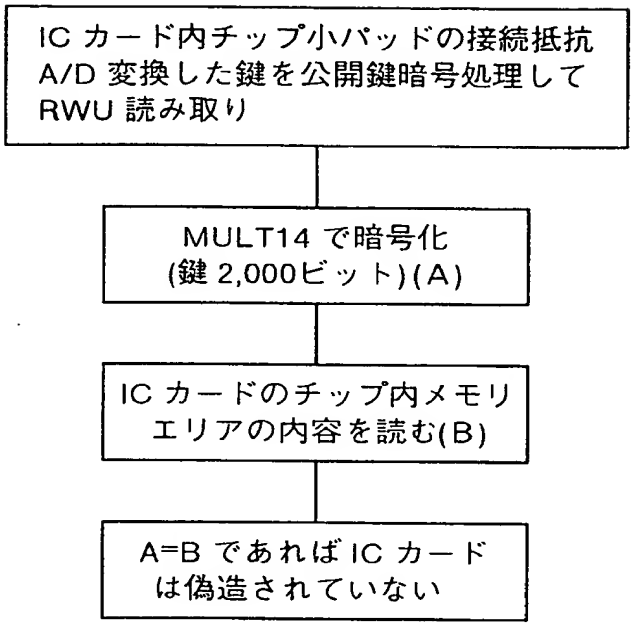
第 5 図


11
51
12
13
14

第 6 図

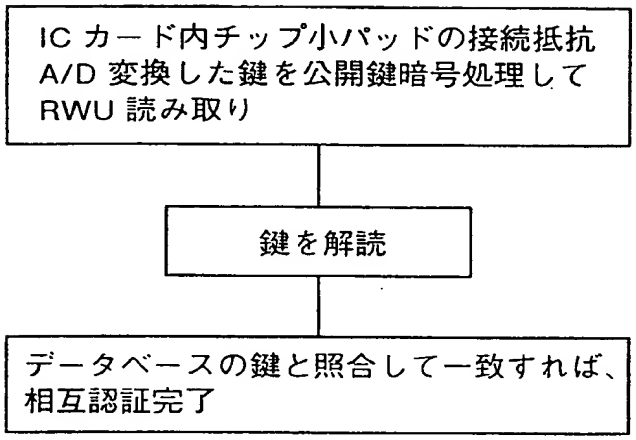


第 7 図

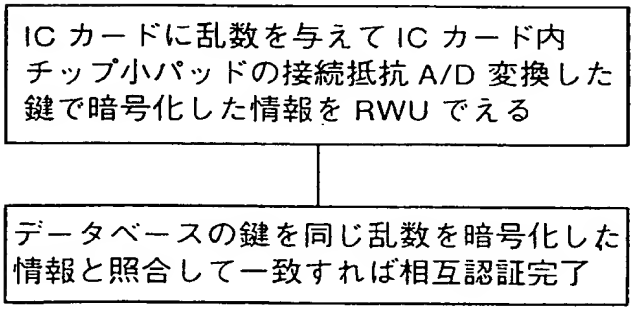

IC カード内チップ小パッドの接続抵抗
A/D 変換した鍵を公開鍵暗号処理して
RWU 読み取り
MULT14 で暗号化
(鍵 2,000ビット)(A)
IC カードのチップ内メモリ
エリアの内容を読む(B)
A=B であれば IC カード
は偽造されていない

第 8 図

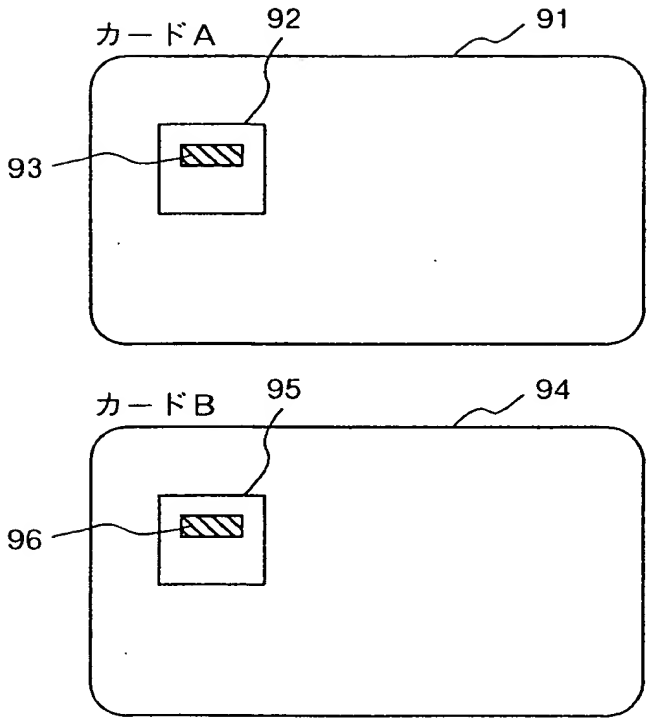
(a)


IC カード内チップ小パッドの接続抵抗
A/D 変換した鍵を公開鍵暗号処理して
RWU 読み取り
鍵を解読
データベースの鍵と照合して一致すれば、
相互認証完了

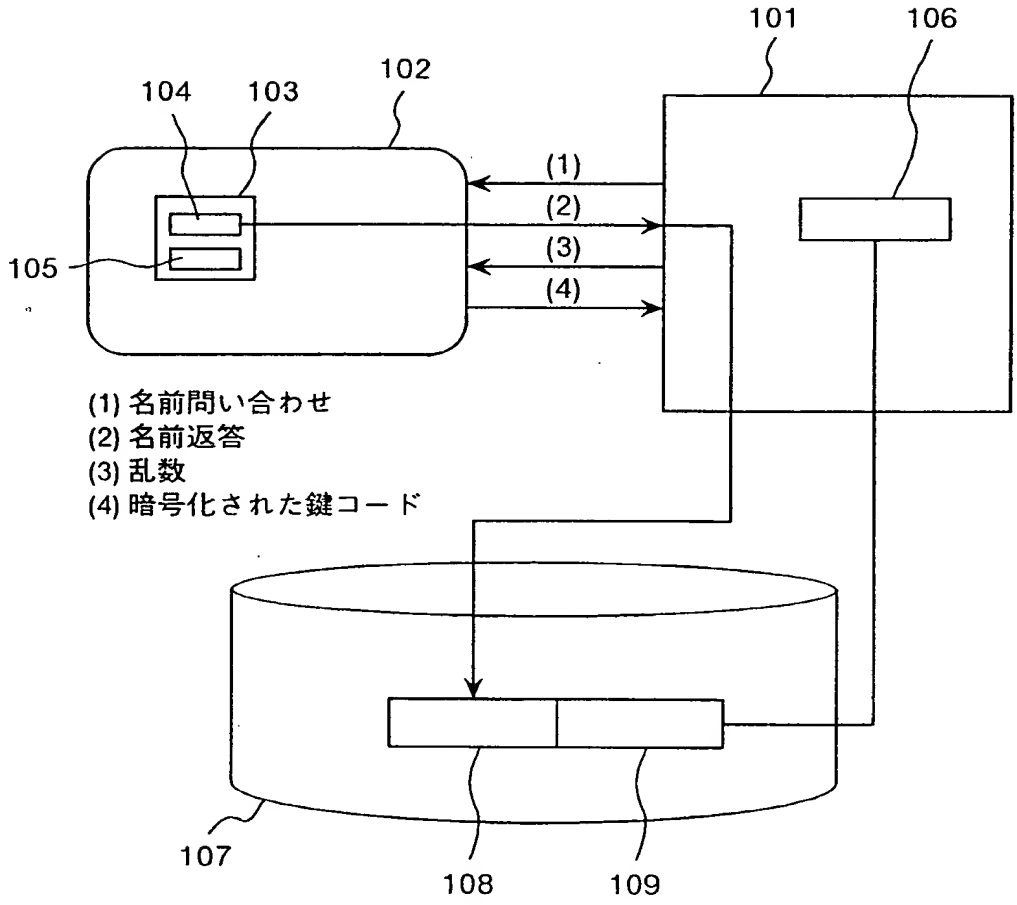
(b)


IC カードに乱数を与えて IC カード内
チップ小パッドの接続抵抗 A/D 変換した
鍵で暗号化した情報を RWU でえる
データベースの鍵を同じ乱数を暗号化した
情報と照合して一致すれば相互認証完了

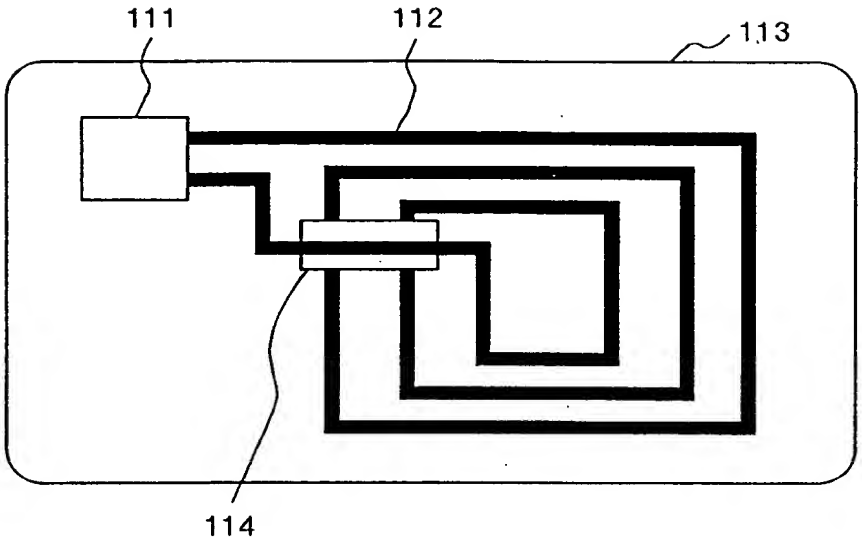
第９図



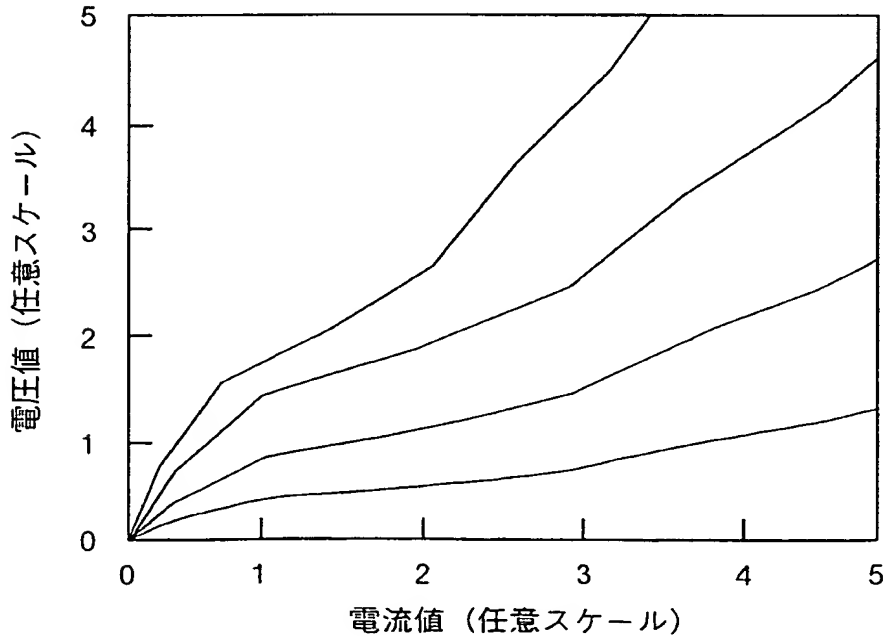
第１０図


101
106
102
104
103
(1)
(2)
(3)
(4)
105
(1) 名前問い合わせ
(2) 名前返答
(3) 乱数
(4) 暗号化された鍵コード
107
108
109

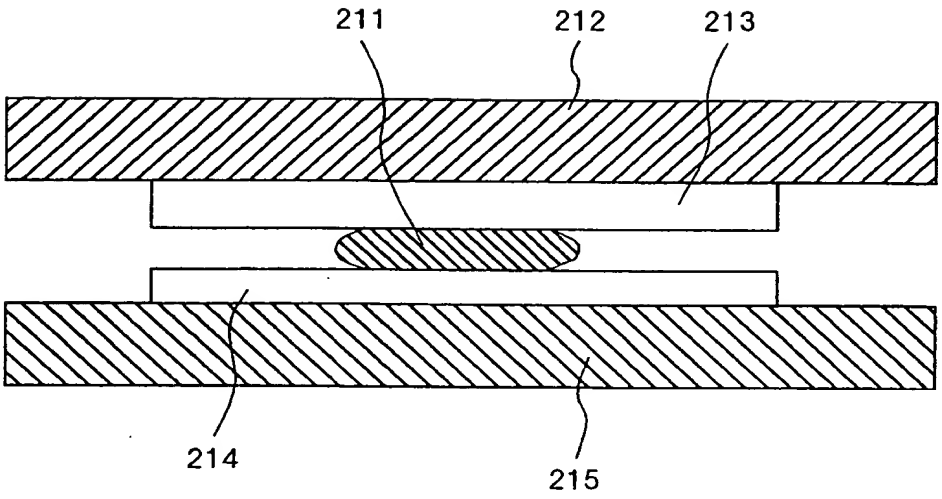
第１１図



第１２図

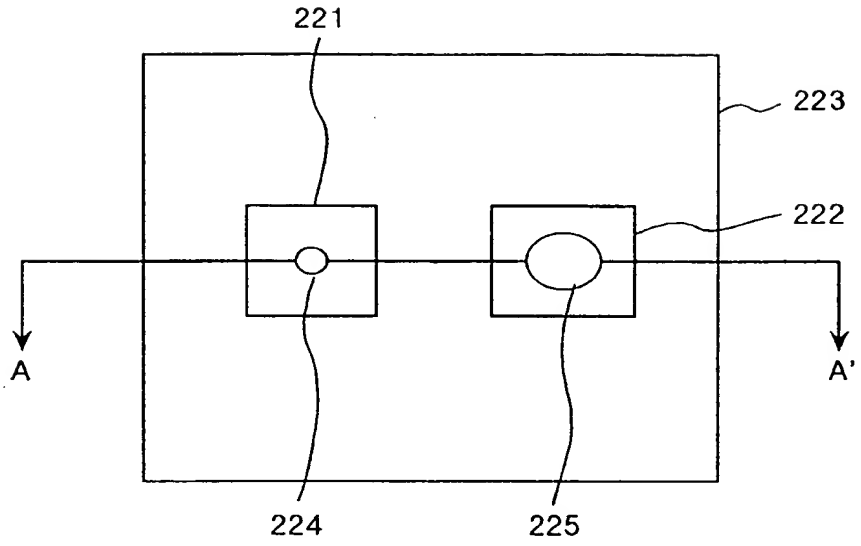


第１３図

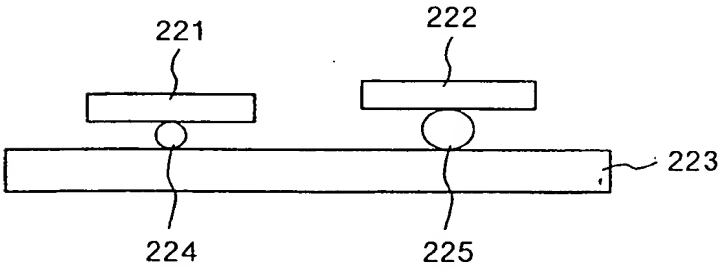


第１４図

（ａ）

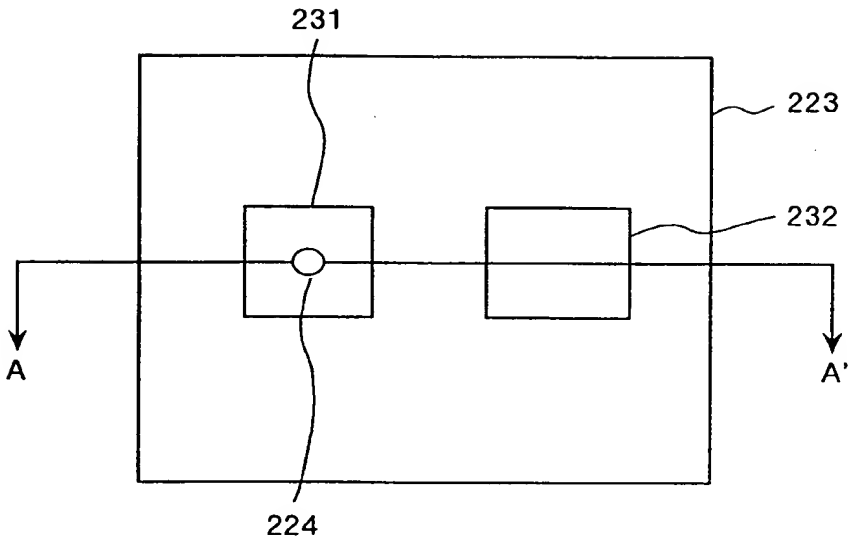


（ｂ）

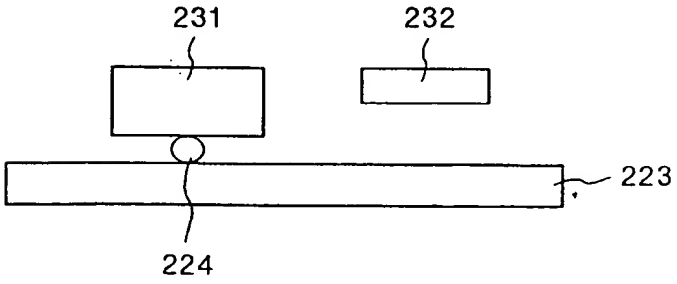


第１５図

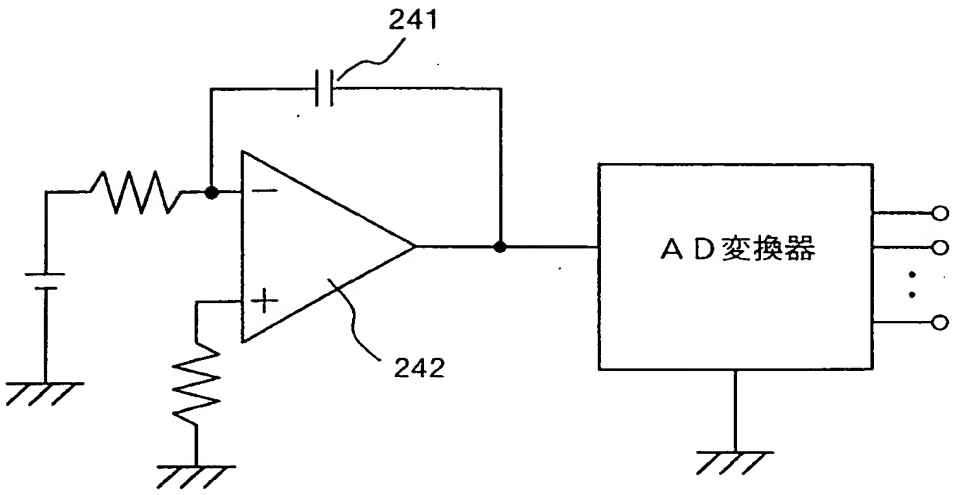
(a)



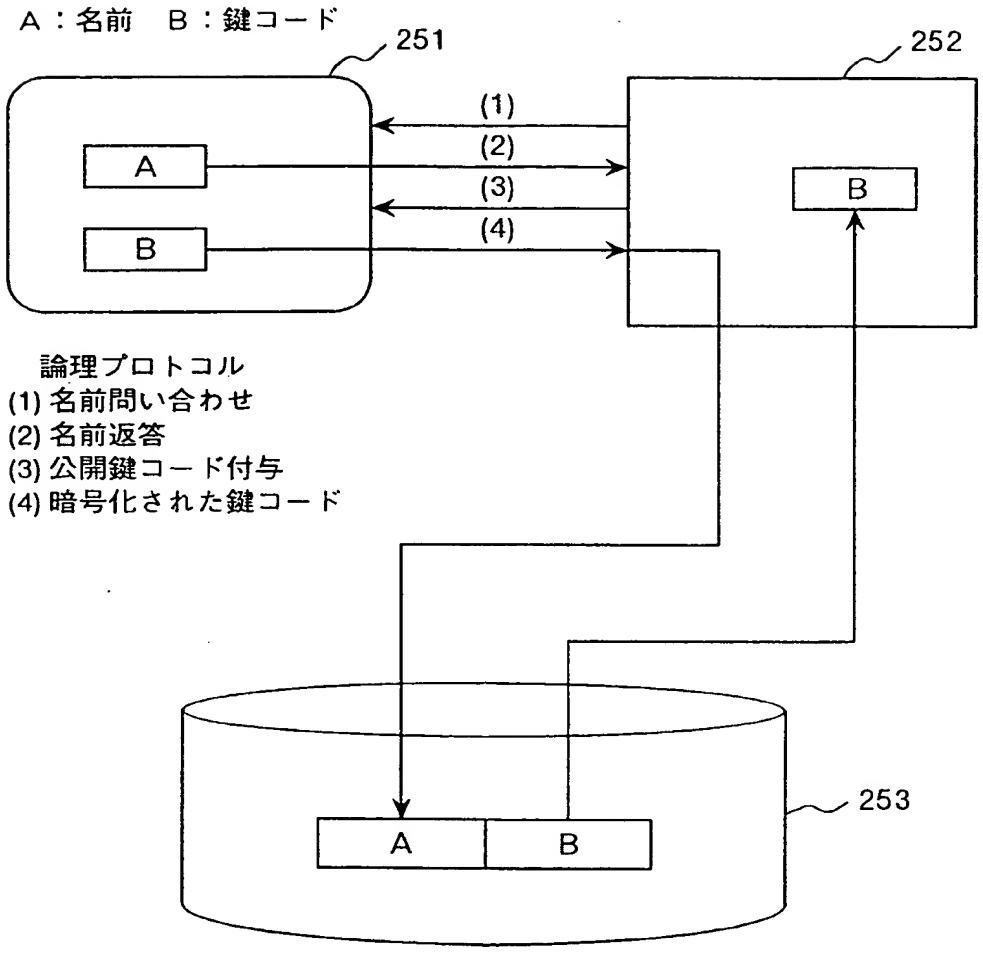
(b)



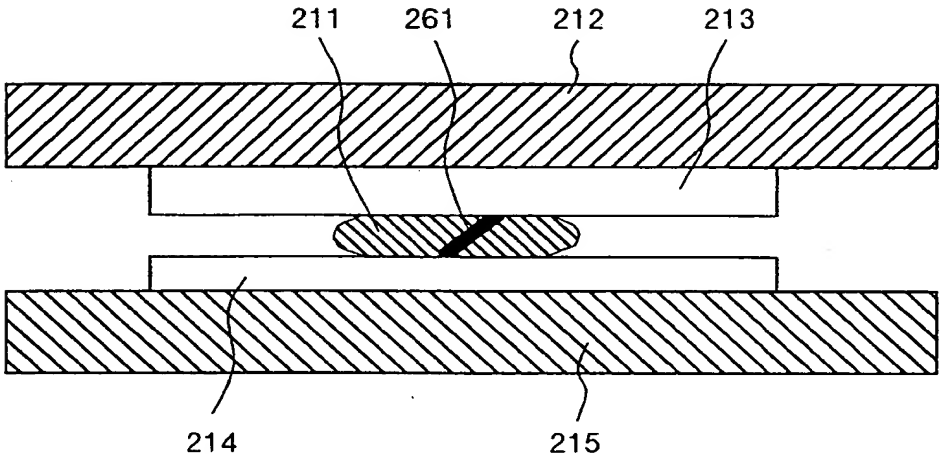
第１６図



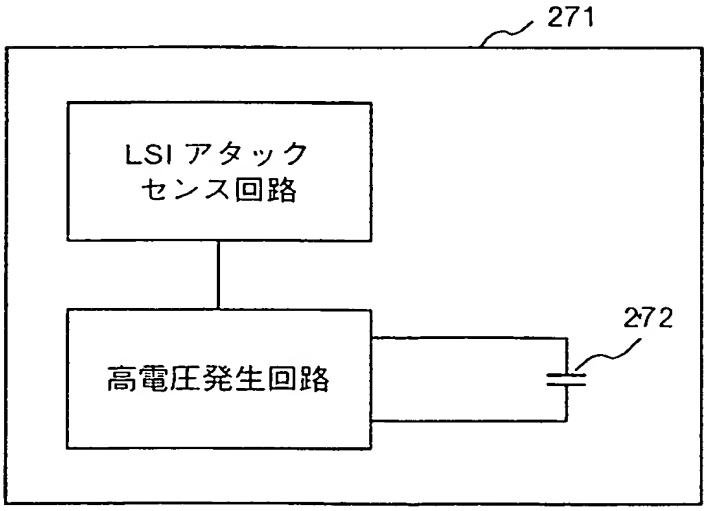
第１７図


A：名前　B：鍵コード
251
252
(1)
(2)
(3)
(4)
A
B
B
論理プロトコル
(1) 名前問い合わせ
(2) 名前返答
(3) 公開鍵コード付与
(4) 暗号化された鍵コード
253
A
B

第１８図

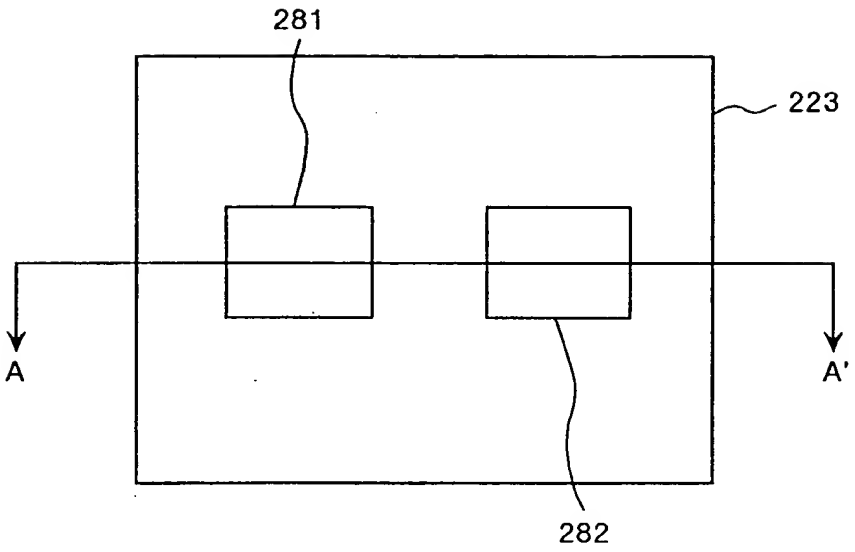


第１９図

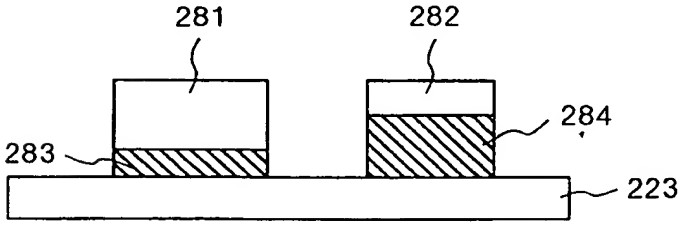


第２０図

(a)



(b)



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/03505

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G06F12/14, G06K19/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G06F12/14, G06K19/07

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1971-1998 Toroku Jitsuyo Shinan Koho 1994-1998
Kokai Jitsuyo Shinan Koho 1971-1994

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 2-501961, A (GAO Gesellshaft für Automation und Organisation mbH.), 28 June, 1990 (28. 06. 90), Page 5, upper left column, line 3 to page 7, upper	1, 5-10, 13-15, 17-35, 44-45
Y	right column, line 5 ; page 10, upper left column, line 21 to page 13, lower left column, line 16	2-3, 11-12
A	& EP, 313967, A1 & WO, 8904033, A1 & DE, 3879616, A1 & HK, 60395, A	4, 16, 36-43
Y	JP, 1-127393, A (Toshiba Corp.), 19 May, 1989 (19. 05. 89) (Family: none)	2, 3
Y	JP, 62-231354, A (Matsushita Electric Industrial Co., Ltd.), 9 October, 1987 (09. 10. 87)	11-12
Y	JP, 4-69791, A (Toshiba Corp.), 4 March, 1992 (04. 03. 92) (Family: none)	12
P	& EP, 800209, A1 & FR, 2746962, A1	1-34

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 November, 1998 (02. 11. 98)	17 November, 1998 (17. 11. 98)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０３５０５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl⁶　Ｇ０６Ｆ１２／１４，Ｇ０６Ｋ１９／０７

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl⁶　Ｇ０６Ｆ１２／１４，Ｇ０６Ｋ１９／０７

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　　１９７１－１９９８年
日本国公開実用新案公報　１９７１－１９９４年
日本国登録実用新案公報　１９９４－１９９８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ，２－５０１９６１，Ａ（ゲーアーオー・ゲゼルシャフト・フューア・アウトマツイオーン・ウント・オルガニザツイオーン・エムベーハー）２８．６月．１９９０（２８．０６．９０）第５頁左上欄第３行～第７頁右上欄第５行、第１０頁左上欄第２１行～第１３頁左下欄第１６行　　＆ＥＰ，３１３９６７，Ａ１　＆ＷＯ，８９０４０３３，Ａ１　＆ＤＥ，３８７９６１６，Ａ１　＆ＨＫ，６０３９５，Ａ	１，５－10，13－15，17－35，44－45
Ｙ		２－３，11－12
Ａ		４，16，36－43
Ｙ	ＪＰ，１－１２７３９３，Ａ（株式会社東芝）１９．５月．１９８９（１９．０５．８９）　（ファミリーなし）	２，３

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」先行文献ではあるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日　０２．１１．９８	国際調査報告の発送日　17.11.98
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｂ　９２９２ 金田　利規 電話番号　０３－３５８１－１１０１　内線　３５４５

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９２年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０３５０５

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，６２－２３１３５４，Ａ（松下電器産業株式会社）９．１０月．１９８７（０９．１０．８７）	１１－１２
Ｙ	ＪＰ，４－６９７９１，Ａ（株式会社東芝）４．３月．１９９２（０４．０３．９２）（ファミリーなし）	１２
Ｐ	＆ＥＰ，８００２０９，Ａ１　＆ＦＲ，２７４６９６２，Ａ１	１－３４